

ABSTRACT

5 A method of enabling authenticated communication of information between at least a primary entity and each of one or more secondary entities, each of the one or more secondary entities having an identifier associated with it, the method including the steps of: allocating first secret information to the primary entity; for each of the one or more secondary entities, determining second secret information, the second secret information being the result of a one way function applied to that second secret entity's identifier and the first secret information; and allocating the second secret information to the or each secondary entity.